UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,684	03/17/2004	Hisanori Kawaura	250480US2	1875

22850 7590 09/21/2007

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
09/21/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/801,684	KAWAURA ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event; however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-12,14-17,19-28 and 30-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-12,14-17,19-28 and 30-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on July 26th , 2007 has been entered. Claims 1, 3-12, 14-17, 19-28, and 30-32 are pending. Claims 1, 12, 17, and 28 are amended by the applicant and claims 2, 13, 18, and 29 are also cancelled by the applicant.

Response to Amendment

Regarding claims 1, 12, 17, and 28:

Applicant has amended the claims to recite the limitation "**wherein the authentication of the update program is performed based on a message digest of a configuration file of the update program and a unique identification of the external source**" it is noted, however, such this limitation was not previously recited in the claims. As such , this limitation is being treated as a newly added limitation and will so examined and argued accordingly (the same).

Applicant argued that the applied prior art fails to disclose the newly added limitation However, upon closer review of the references, it is submitted that the prior art of the record discloses such feature. "Firmware updates are then distributed to the devices so as to define the functions of the device based on an authorization associated with the device (block 712). Such authorization may be provided, for example, by identifying a serial number, MAC address license key or other identifier associated with the device, which may be used to provide authorization to the device to update the firmware of the device to provide the authorized functionality "(column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60)

First, Applicant is respectfully reminded that during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." (Phillips v. AWH Corp., 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005)). See MPEP 2111.

On pages, 12, 13, and 14 of the reply, Applicant argued that the applied prior art fails to disclose the newly added limitation. Applicant further encloses that " As disclosed in an exemplary embodiment at p. 21, lines 8-20 of the specification, a serial number of a memory card, which acts as an external source of the update program, is a portion of the information used to authenticate a received update program. Thus, a unique identification (e.g., serial number) of the extemal source (e.g., memory card) from which the update program is acquired is used to authenticate the received update program."

However, **Kutaragi et al** (US 2002/0120722) discloses such a feature (Fig.1, paragraphs [0016], [0026]).

Therefore dependant claims 3-11, 14-16, 19-27, and 30-32 are also rejected based on the above argument.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-11, 16, 19-27, 32 rejected under 35 U.S.C. 103(a) as being unpatentable over **Hind et al** (US 6976163) in view of **Kutaragi et al** (US 2002/0120722).

Claim 1: **Hind et al** discloses an apparatus for secure firmware update comprising:

a. A storing unit configured to store a program in accordance with which the image forming apparatus operates (the computer program instructions is stored in a computer- readable memory that directs a computer or other programmable data processing apparatus to function in a particular manner) (column 6, lines 36-40); An acquiring unit configured to acquire an update program from an external source (the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process) (column 6, lies 44-48; Fig. 3, Fig. 4, Fig. 10); and

b. An updating unit that determines whether an electronic signature of the update program acquired by said acquiring unit is authentic and, if the electronic signature of the acquired update program is determined to be authentic (the authenticity of the update image is verified. Such verification is accomplish in various ways for example by including a and checking a digital signature comprising a hash of the image encrypted by the private key of the an update authority) (column 3, lines 18-30), updates the program stored in said storing unit using the acquired update program (the programmable memory is updated with

the update image only if all the update application rules indicate that the update image is applicable to the device) (column 2, lines 53-60).

c. Wherein the authentication of the update program is performed based on a message digest of a configuration file of the update program (the sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed) (column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60).

But **Hind et al** does not explicitly disclose that the authentication of the update program is performed based on a unique identification of the external source. However, **Kutaragi et al** discloses an apparatus enabling mutual exchange of information between users and digital contents, which further discloses that the authentication of the update program is performed based on a unique identification of the external source (Fig. 1 paragraphs [0016], [0026]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to Hind et al to include a step of authentication based on the identification of the external source. One would haven been motivated to do so in order to verify the integrity of the source of the update program.

Claim 17: **Hind et al** discloses an apparatus for secure firmware updates comprising:

a. A storing unit that stores a program in accordance with which the image forming apparatus operates (the computer program instructions is stored in a computer- readable memory that directs a computer or other programmable data

processing apparatus to function in a particular manner) (column 6, lines 36-40); An acquiring unit that acquires an update program from an external source (the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process) (column 6, lies 44-48); and

b. An updating unit that updates the program stored in said storing unit using the update program acquired by said acquiring unit, wherein after updating the program stored in said storing unit, said updating unit determines whether an electronic signature of the updated program is authentic and, if the electronic signature of the updated program is authentic (the authenticity of the update image is verified. Such verification is accomplish in various ways for example by including a and checking a digital signature comprising a hash of the image encrypted by the private key of the an update authority) (column 3, lines 18-30), said updating unit maintains the updated program (the programmable memory is updated with the update image only if all the update application rules indicate that the update image is applicable to the device) (column 2, lines 53-60).

c. Wherein the authentication of the update program is performed based on a message digest of a configuration file of the update program (the sender encrypts a signature message using the sender's private key , the signature messing being a hash or a message digest of the message being signed)

(column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60)

But **Hind et al** does not explicitly disclose that the authentication of the update program is performed based on a unique identification of the external source. However, **Kutaragi et al** discloses an apparatus enabling mutual exchange of information between users and digital contents, which further discloses that the authentication of the update program is performed based on a unique identification of the external source (Fig. 1 paragraphs [0016], [0026]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to Hind et al to include a step of authentication based on the identification of the external source. One would haven been motivated to do so in order to verify the integrity of the source of the update program.

Claims 3, 19: **Hind et al** and **Kutaragi et al** discloses an apparatus for secure firmware updates as in claims 1 and 17 above, and **Hind et al** further discloses that said updating unit updates the program stored in said storing unit with the update program acquired by said acquiring unit, and updates an electronic signature of the program stored in said storing unit with the electronic signature of the update program (the update application rules defines how data from the update image is utilized to update the programmable memory and identifies installation information provided with the update image. The programmable memory would be updated utilizing the installation information by executing the install program to write the update data to the programmable memory) (column 3, lines 5-17).

Claims 4, 20: **Hind et al** and **Kutaragi et al** discloses an apparatus for secure firmware updates as in claims 1 and 17 above, and **Hind et al** further discloses that said acquiring unit is an update recording medium setting unit and the external source is an update recording medium to be set in the update recording medium setting unit, the update recording medium storing the update program and the electronic signature of the update program (any suitable computer readable medium may be utilized including hard disk, CD-ROMs, optical storage devices, or magnetic storage devices) (column 5, lines50-53).

Claims 5, 21: **Hind et al** and **Kutaragi et al** discloses an apparatus for secure firmware updates as in claims 1 and 17 above, and **Hind et al** further discloses that said acquiring unit is a receiving unit that receives the update program and the electronic signature of the update program from the external source via a network (the computer program is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be perfume on the computer) (column 6, lines 44-48).

Claims 6, 22: **Hind et al** and **Kutaragi et al** discloses an apparatus for secure firmware updates as in claims 1 and 17 above, and **Hind et al** further discloses that said storing unit further comprises a recording medium setting unit and a recording medium set therein, the recording medium storing the program (these computer program instructions are also stored in a computer readable memory that can direct a computer and other programmable data processing apparatus to function in a particular manner) (column 6, lines 36-39).

Claims 7, 23: **Hind et al** and **Kutaragi et al** disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and **Hind et al** further discloses:

An activating unit that determines whether the electronic signature of the update program and an electronic signature of a configuration file related to the update program are authentic and, if the electronic signature of the update program and the electronic signature of the configuration file related to the update program are determined to be authentic, activates the updated program (the update image includes a plurality of certificates in a hierarchy of certificates. Authenticity of the update image is verified by evaluating each of the plurality of certificates in the update image to determine if a valid digital signature is provide with each certificate of the update image (update program and configuration file) (column 4, lines 4-10),

Wherein said acquiring unit further acquires a configuration file and an electronic signature thereof from the external source (the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process) (column 6, lies 44-48); and said activating unit determines whether the electronic signature of the update program and the electronic signature of the configuration file are authentic and, if the electronic signature of the update program and the electronic signature of the configuration file are determined to be authentic, activates the update program in accordance with the configuration file (the invention also provide a certificate for use in updating a programmable memory. Such certificate includes a digital signature and at least one

extension having rules to control installation of an update image. A private key of a certificate authority signs the certificate. The programmable memories of generic processing devices is selectively update based on the distributed updates and the rules specified in the at least extension of the certificate. The sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed) (column 12, lines 1-14, column , 12, lines 12-22).

Claims 8, 24: **Hind et al** and **Kutaragi et al** disclose an apparatus for secure firmware updates as in claims 7 and 23 above, and **Hind et al** further discloses that said activating unit determines whether the electronic signature of the update program is authentic by comparing a message digest generated from the update program and a message digest obtained by decrypting the electronic signature of the update program (the verification of signature is provided by computing the hash over the image, decrypting the signature using the public key from the included certificate, and comparing the decrypt result with the computed hash value) (column 3, lines 33-36).

Claims 9, 25: **Hind et al** and **Kutaragi et al** disclose an apparatus for secure firmware updates as in claims 7 and 23 above, and **Hind et al** further discloses that said activating unit determines whether the electronic signature of the configuration file is authentic by comparing a message digest generated from the configuration file and a message digest obtained by decrypting the electronic signature of the configuration file (the verification of signature is provided by computing the hash over the image,

decrypting the signature using the public key from the included certificate, and comparing the decrypt result with the computed hash value) (column 3, lines 33-36).

Claims 10, 26: **Hind et al** and **Kutaragi et al** disclose an apparatus for secure firmware updates as in claims 9 and 25 above, **Hind et al** further discloses that that the electronic signature of the configuration file is generated by encrypting a message digest of the configuration file and identification information of the recording medium (the sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed) (column 12, lines 1-14, column , 12, lines 12-22)

Claims 11, 27: **Hind et al** and **Kutaragi et al** disclose an apparatus for secure firmware updates as in claims 10 and 26 above, and **Kutaragi et al** further discloses that the identification information of the recording medium iis a serial ID of the recording medium. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made **to Hind et al** to include a step of authentication based on the identification of the external source. One would haven been motivated to do so in order to verify the integrity of the source of the update program.

Claims 16, 32: **Hind et al** and **Kutaragi et al** discloses an apparatus for secure firmware updates as in claims 4 and 20 above, and **Hind et al** further discloses that the update recording medium storing the update program and the electronic signature thereof (the update application rules defines how data from the update image is utilized to update the programmable memory and identifies installation information provided with the update image. The programmable memory would be updated utilizing the

installation information by executing the install program to write the update data to the programmable memory) (column 3, lines 5-17).

4. Claims 12, 14, 15, 28, 30, 31 rejected under 35 U.S.C. 103(a) as being unpatentable over **Mattison** (US 6615355) in view of **Kutaragi et al** (US 2002/0120722).

Claim 12: **Mattison** discloses a method for protecting flash memory from any unauthorized reprogramming effort comprising:

a. Acquiring an update program and an electronic signature corresponding to the update program (a flash memory upgrade program containing a new flash memory image for the flash memory would be loaded into main system memory) (column 3, lines 25-27); Determining whether the acquired electronic signature of the update program is authentic (comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match) (column 3, lines 51-54); and

b. Updating, if the acquired electronic signature of the acquired update program is determined to be authentic, the program stored in the recording medium using the acquired update program (if the hash values match, indicating that flash memory upgrade program containing in main memory originated from the authorized creator and has not been modified, then the current program containing in the lash memory would enable reprogramming of the flash memory

and return control of the processor to the flash memory upgrade program) (column 3, lines 55-61).

c. Wherein the authentication of the update program is performed based on a message digest of a configuration file of the update program (a signature is generated for a block of information by a sender generating a hash value with the sender's private key. That, the encrypted hash value is the signature of the vendor for that block of information) (column 5; lines 25-55, column 8; lines 1-10, column 9; and lines 40-50).

But **Mattison** does not explicitly disclose that the authentication of the update program is performed based on a unique identification of the external source. However, **Kutaragi et al** discloses an apparatus enabling mutual exchange of information between users and digital contents, which further discloses that the authentication of the update program is performed based on a unique identification of the external source (Fig. 1 paragraphs [0016], [0026]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to **Matisson** to include a step of authentication based on the identification of the external source. One would haven been motivated to do so in order to verify the integrity of the source of the update program.

Claim 28: **Mattison** discloses a method for protecting flash memory from any unauthorized reprogramming effort comprising:

Acquiring an update program from an external source (a flash memory upgrade program containing a new flash memory image for the flash memory would be loaded into main system memory) (column 3, lines 25-27);

Updating the program stored in the recording medium using the acquired update program (the flash memory upgrade would then erase the flash memory and copy the new flash memory image into the flash memory) (column 3. lines 62-64);

Determining whether an electronic signature of the updated program is authentic (comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match) (column 3, lines 51-54); and maintaining, if the electronic signature of the updated program is determined to be authentic, the updated program (if the hash values match, indicating that flash memory upgrade program containing in main memory originated from the authorized creator and has not been modified, then the current program containing in the lash memory would enable reprogramming of the flash memory and return control of the processor to the flash memory upgrade program) (column 3, lines 55-61).

But **Mattison** does not explicitly disclose that the authentication of the update program is performed based on a unique identification of the external source. However, **Kutaragi et al** discloses an apparatus enabling mutual exchange of information between users and digital contents, which further discloses that the authentication of the update program is performed based on a unique identification of the external source

(Fig. 1 paragraphs [0016], [0026]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to **Matisson** to include a step of authentication based on the identification of the external source. One would haven been motivated to do so in order to verify the integrity of the source of the update program.

Claims 14, 30: **Mattison** and **Kutaragi et al** disclose a method for protecting flash memory from any unauthorized reprogramming as in claims 12 and 28, and further discloses that if the step of acquiring electronic signature of the update program is determined to be authentic, an electronic signature of the program stored in the recording medium is updated together with the program stored in the recording medium (the flash memory upgrade would then erase the flash memory and copy the new flash memory image into the flash memory) (column 3. lines 62-64).

Claims 15, 31: **Mattison** and **Kutaragi et al** disclose a method for protecting flash memory from any unauthorized reprogramming effort as claimed in claims 12 and 28 above, which further comprises a step of activating, if the acquired electronic signature of the acquired update program and an acquired electronic signature of an acquired configuration file are determined to be authentic, the updated program in accordance with the acquired configuration file (the flash memory upgrade program, still executing from main system memory, would then transfer control of the processor to the program containing in the new flash memory image, now in flash memory, which in turn would return the memory controller to normal operation and begin its normal initialization sequence as if a reset had occurred) (column 4, lines 13-20).

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

FT
Monday, September 17, 2007

Nassar G. Moazzami
Supervisory Patent Examiner

9/17/07